



DPC: 23 / 30471808 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 21 March 2023

Origin: International

Latest date for receipt of comments: 12 April 2023

Project No. 2017/02526

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: BS EN IEC/IEEE 60802 Time-sensitive networking profile for industrial automation

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 12 April 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: Ms Charmaine Mukherjee (BSI)

Direct tel:

E-mail: charmaine.mukherjee@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



65C/1251/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC/IEEE 60802 ED1

DATE OF CIRCULATION:

2023-03-17

CLOSING DATE FOR COMMENTS:

2023-05-12

SUPERSEDES DOCUMENTS:

65C/1116/CD, 65C/1135A/CC

IEC SC 65C : INDUSTRIAL NETWORKS

SECRETARIAT:

France

SECRETARY:

Ms Valérie DEMASSIEUX

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 57

PROPOSED HORIZONTAL STANDARD:



Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of

- any relevant patent rights of which they are aware and to provide supporting documentation,
- any local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "in some countries" clauses. See AC/22/2007.

TITLE:

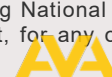
Time-sensitive networking profile for industrial automation

NOTE FROM TC/SC OFFICERS:

This fifth CD of the joint IEC/IEEE 60802 project is circulated in parallel with an IEEE 802.1 initial WG ballot.

If your NC submits comments through the IEEE system, please avoid duplication of these comments through the IEC system.

Copyright © 2023 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.



Documents

Document Sharing Hub

CONTENTS

FOREWORD	7
INTRODUCTION	9
1 Scope	10
2 Normative References	10
3 Terms, definitions, symbols, abbreviated terms and conventions	13
3.1 General	13
3.2 List of terms, abbreviated terms and definitions given in various standards	13
3.3 Terms defined in this document	15
3.4 Abbreviated terms and acronyms	17
3.5 Conventions	20
3.5.1 Principles for (sub) clause selections of referenced documents	20
3.5.2 Convention for capitalizations	20
3.5.3 Unit conventions	20
3.5.4 Conventions for YANG contents	20
4 Overview of TSN in industrial automation	21
4.1 Industrial application operation	21
4.2 Industrial applications	22
4.2.1 General	22
4.2.2 Control loop tasks	24
4.2.3 Start of control loop tasks	25
4.3 IA-stations	25
4.4 Ethernet interface	25
4.5 Mechanisms that can be used to meet control loop latency requirements	26
4.6 Translation between middleware and network provisioning	27
4.6.1 Interfaces of type I2vlan	27
4.6.2 PTP Instances	28
4.7 Industrial traffic types	30
4.7.1 General	30
4.7.2 Traffic type characteristics	30
4.7.3 Traffic type categories	30
4.7.4 Traffic types	31
4.8 Security for TSN-IA	33
4.8.1 General	33
4.8.2 Security configuration model	33
4.8.3 NETCONF/YANG processing	34
4.8.4 NETCONF/YANG access control	35
4.8.5 Identity checking	36
4.8.6 Secure device identity	37
5 Conformance	39
5.1 General	39
5.2 Requirements terminology	39
5.3 Profile conformance statement (PCS)	40
5.4 Conformance classes	40
5.5 IA-station requirements	40
5.5.1 IA-station PHY and MAC requirements for external ports	40

48	5.5.2	IA-station topology discovery requirements.....	41
49	5.5.3	IA-station requirements for time synchronization.....	41
50	5.5.4	IA-station requirements for security	42
51	5.5.5	IA-station requirements for management	42
52	5.5.6	IA-station requirements for digital data sheet.....	43
53	5.6	IA-station options.....	43
54	5.6.1	IA-station PHY and MAC options for external ports	43
55	5.6.2	IA-station options for time synchronization.....	44
56	5.6.3	IA-station options for security	44
57	5.6.4	IA-station options for management	44
58	5.7	Bridge component requirements.....	45
59	5.7.1	Common Bridge component requirements	45
60	5.7.2	ccA Bridge component requirements.....	45
61	5.7.3	ccB Bridge component requirements.....	46
62	5.8	Bridge component options.....	46
63	5.8.1	Common Bridge component options.....	46
64	5.8.2	ccA Bridge component options.....	46
65	5.8.3	ccB Bridge component options.....	47
66	5.9	End station component requirements	47
67	5.9.1	Common End Station Component Requirements.....	47
68	5.9.2	ccA end station component requirements	48
69	5.9.3	ccB end station component requirements	48
70	5.10	End station component options	48
71	5.10.1	Common end station component options	48
72	5.10.2	ccA end station component options	49
73	5.10.3	ccB end station component options	49
74	5.11	CNC requirements	49
75	5.12	CNC options	50
76	5.13	CUC requirements	50
77	6	Required functions for an industrial network	50
78	6.1	General.....	50
79	6.2	Synchronization	50
80	6.2.1	General	50
81	6.2.2	PTP Instance requirements.....	50
82	6.2.3	PTP protocol requirements	51
83	6.2.4	Clock states.....	54
84	6.2.5	Grandmaster PTP Instance requirements	55
85	6.2.6	Application framework	55
86	6.2.7	Working Clock domain framework.....	56
87	6.2.8	Global Time domain framework	57
88	6.2.9	IA-station model for clocks.....	57
89	6.2.10	Clock usage for the Ethernet interface.....	59
90	6.2.11	Error model	60
91	6.2.12	gPTP domains and PTP Instances.....	61
92	6.2.13	Split and combine cases for a PTP domain.....	61
93	6.3	Security model.....	63
94	6.3.1	General	63
95	6.3.2	Security functionality	64
96	6.3.3	IDeVID Profile	66

97	6.3.4	Security setup based on IDevID.....	70
98	6.3.5	Secure configuration based on LDevID-NETCONF	74
99	6.4	Bridge delay Requirements	74
100	6.5	Bridge FDB requirements.....	74
101	6.6	Bridge reporting requirements.....	75
102	6.7	Management.....	75
103	6.7.1	General	75
104	6.7.2	IA-station management model	75
105	6.7.3	Discovery of IA-station internal structure	80
106	6.7.4	Network engineering model	80
107	6.7.5	Operation	84
108	6.7.6	Engineered time-synchronization spanning tree.....	90
109	6.7.7	Diagnostics.....	92
110	6.7.8	Data sheet.....	94
111	6.7.9	YANG representation of managed objects	96
112	6.8	Topology discovery and verification	109
113	6.8.1	Topology discovery and verification requirements.....	109
114	6.8.2	Topology discovery overview	110
115	6.8.3	Topology verification overview.....	112
116	6.9	CNC.....	112
117	6.9.1	General	112
118	6.9.2	Stream destination MAC address range.....	112
119	Annex A (normative) PCS proforma – Time-sensitive networking profile for industrial automation		114
120			
121	A.1	General.....	114
122	A.2	Abbreviations and special symbols	114
123	A.2.1	Status symbols	114
124	A.2.2	General abbreviations.....	114
125	A.3	Instructions for completing the PCS proforma	115
126	A.3.1	General structure of the PCS proforma	115
127	A.3.2	Additional information	115
128	A.3.3	Exception information	115
129	A.3.4	Conditional status.....	116
130	A.3.5	Electronic datasheet.....	116
131	A.4	Common requirements.....	117
132	A.4.1	Implementation identification	117
133	A.4.2	Profile summary, IEC/IEEE 60802	117
134	A.4.3	Implementation type	117
135	Annex B (informative) Representative Configuration Domain		118
136	Annex C (informative) Error model.....		119
137	C.1	General.....	119
138	C.2	Time error components due to relaying of time.....	119
139	C.3	Time error components due to providing time to the Grandmaster or to an end application	120
140			
141	Annex D (informative) Description of Clock Control System		121
142	D.1	Introduction.....	121
143	D.2	Transfer function for control system	122
144	D.3	Frequency response for control system.....	123
145	D.4	Example	128

146	Annex Z (informative) Gaps	130
147	Z.1 Gaps for Release 1:	130
148	Z.2 Topics for Edition 2:	131
149	Bibliography	132
150		
151	Figure 1 – Data flow in a control loop	21
152	Figure 2 – IA-station interaction with CNC – Transmit path	23
153	Figure 3 – IA-station interaction with CNC – Receive path	24
154	Figure 4 – IA-station example	25
155	Figure 5 – Model for cycles	26
156	Figure 6 – Traffic type translation example	27
157	Figure 7 – IETF Interfaces used for Traffic Type Translation	28
158	Figure 8 – PTP Instance Translation Example	29
159	Figure 9 – IETF Interfaces used for PTP Instance Translation	29
160	Figure 10 – NETCONF/YANG security processing steps	35
161	Figure 11 – IA-station conformance model	40
162	Figure 12 – Externally controlled ClockSource of a Grandmaster	55
163	Figure 13 – Clock states	56
164	Figure 14 – Example clock usage principles for PTP End Instances	58
165	Figure 15 – Example clock usage principles for Grandmaster PTP Instances	59
166	Figure 16 – Error budget scheme	60
167	Figure 17 – Split and combine using BMCA	62
168	Figure 18 – Split and combine using hot standby	63
169	Figure 19 – Generic IEEE 802.1Q YANG Bridge management model	76
170	Figure 20 – Internal LAN connection management model	76
171	Figure 21 – IA-station example with IETF interfaces	77
172	Figure 22 – VID/FID/MSTID example	78
173	Figure 23 – Structure and interfaces of a CNC	82
174	Figure 24 – IA-station structure example	83
175	Figure 25 – CNC interaction	83
176	Figure 26 – Operational management model	84
177	Figure 27 – UNI service model	85
178	Figure 28 – CNC southbound	85
179	Figure 29 – NETCONF usage in a configuration domain	86
180	Figure 30 – Boundary port model	87
181	Figure 31 – Observer model	93
182	Figure 32 – Creation of the digital data sheet of an IA-station	96
183	Figure 33 – Usage example of LLDP	110
184	Figure 34 – Stream Destination MAC Address	113
185	Figure D.1 – Reference model for clock control system	121
186	Figure D.2 – Frequency response for the control system of Figure D.1, for damping	
187	ratio equal to 0,3, 0,5, 0,707, 1,0, 2,0, 3,0, 4,0, and 5,0	124
188	Figure D.3 – Detail of frequency response for the control system of Figure D.1 for	
189	dimensionless frequency in the range 0,1 to 10	

190	Figure D.4 – Gain peaking, expressed as a pure fraction, as a function of damping	
191	ratio 127	
192	Figure D.5 – Gain peaking in dB as a function of damping ratio	128
193	Figure D.6 – Example Frequency response.....	129
194		
195	Table 1 – List of terms	13
196	Table 2 – Traffic type characteristics	30
197	Table 3 – IA time-aware stream characteristics.....	31
198	Table 4 – IA stream characteristics	31
199	Table 5 – IA traffic engineered non-stream characteristics	31
200	Table 6 – IA non-stream characteristics	31
201	Table 7 – Industrial automation traffic types summary.....	31
202	Table 8 – Example traffic class to traffic type mapping.....	33
203	Table 9 – Required values	51
204	Table 10 – Protocol settings	51
205	Table 11 – Error generation limits for Grandmaster PTP Instance	52
206	Table 12 – Error generation limits for PTP Relay Instance	52
207	Table 13 – Error generation limits for PTP End Instance	54
208	Table 14 – Error budget.....	61
209	Table 15 – gPTP domains.....	61
210	Table A.1 – Implementation identification template	117
211	Table A.2 – Profile summary template.....	117
212	Table A.3 – Implementation type template	117
213		
214		

Time-sensitive networking profile for industrial automation

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC document(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation.

IEEE Standards documents are developed within IEEE Societies and Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of IEEE and serve without compensation. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards. Use of IEEE Standards documents is wholly voluntary. *IEEE documents are made available for use subject to important notices and legal disclaimers (see <https://standards.ieee.org/ipr/disclaimers.html> for more information).*

IEC collaborates closely with IEEE in accordance with conditions determined by agreement between the two organizations. This Dual Logo International Standard was jointly developed by the IEC and IEEE under the terms of that agreement.

2) The formal decisions of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees. The formal decisions of IEEE on technical matters, once consensus within IEEE Societies and Standards Coordinating Committees has been reached, is determined by a balanced ballot of materially interested parties who indicate interest in reviewing the proposed standard. Final approval of the IEEE standards document is given by the IEEE Standards Association (IEEE SA) Standards Board.

3) IEC/IEEE Publications have the form of recommendations for international use and are accepted by IEC National Committees/IEEE Societies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC/IEEE Publications is accurate, IEC or IEEE cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications (including IEC/IEEE Publications) transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC/IEEE Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and IEEE do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC and IEEE are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or IEEE or their directors, employees, servants or agents including individual experts and members of technical committees and IEC National Committees, or volunteers of IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board, for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC/IEEE Publication or any other IEC or IEEE Publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that implementation of this IEC/IEEE Publication may require use of material covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. IEC or IEEE shall not be held responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patent Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

IEC/IEEE 60802 was prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation, in cooperation with IEEE 802.1: Higher Layer LAN Protocols Working Group of IEEE 802: LAN/MAN Standards Committee of the IEEE computer society, under the IEC/IEEE Dual Logo Agreement between IEC and IEEE. It is an International Standard.

280 This document is published as an IEC/IEEE Dual Logo standard.

281 The text of this International Standard is based on the following IEC documents:

Draft	Report on voting
XX/XX/FDIS	XX/XX/RVD

282
283 Full information on the voting for its approval can be found in the report on voting indicated in
284 the above table.

285 The language used for the development of this International Standard is English.

286 This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2,
287 available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC
288 are described in greater detail at www.iec.ch/publications/.

289 The IEC Technical Committee and IEEE Technical Committee have decided that the contents
290 of this document will remain unchanged until the stability date indicated on the IEC website
291 under webstore.iec.ch in the data related to the specific document. At this date, the document
292 will be

- 293 • reconfirmed,
- 294 • withdrawn,
- 295 • replaced by a revised edition, or
- 296 • amended.

297

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

298

299

300

301

INTRODUCTION

Editor's note: This profile has been drafted per the IEC style guide. The use of introductory boilerplate text, editorial conventions and clause numbering may differ from those outlined in the IEEE style guide.

For the convenience of the reviewer, references to the IEC/IEEE cooperation process and to the IEC organization and style guidelines are listed below:

IEC-IEEE 60802 Joint Project Cooperation Process:

<http://www.ieee802.org/1/files/public/docs2018/admin-IEC-IEEE-JWG-cooperation-process-0118.pdf>

IEC organization:

<http://www.iec.ch/>

Home of the IEC organization of the Joint Project IEC/IEEE 60802 is: IEC 65C/WG18:

https://www.iec.ch/dyn/www/f?p=103:14:506767825234046:::FSP_ORG_ID,FSP_LANG_ID:26299,25Assistance to experts drafting IEC documents:

<http://www.iec.ch/standardsdev/resources/draftingpublications/>

Reference material:

http://www.iec.ch/members_experts/refdocs/

ISO/IEC Directives, Part 2:2021

edition 9.0 (2021-05)

Principles and rules for the structure and drafting of ISO and IEC documents:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir2%7Bed9.0%7Den.pdf

ISO/IEC Directives, Part 1:2021 + IEC Supplement:2021 edition 17.0 (2021-05) consolidated with IEC Supplement, edition 15.0 (2021-05) contains the redline version

Procedures for the technical work - Procedures specific to IEC:

https://www.iec.ch/members_experts/refdocs/iec/isoiecdir1-consolidatedIECsup%7Bed17.0%7Den.pdf

This document defines a Time-Sensitive Networking profile for industrial automation. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks.

The profile meets the industrial automation market objective of converging Operations Technology (OT) and Information Technology (IT) networks by defining a common, standardized network infrastructure. This objective is accomplished by taking advantage of the improvements that Time-Sensitive Networking provides to IEEE 802.1 and IEEE 802.3 standard Ethernet networks by providing guaranteed data transport with bounded low latency, low latency variation, zero congestion loss for critical traffic, and high availability.

The profile helps the convergence of industrial communication networks by referring only to international standards to build the lower layers of the communication stack and their management.

Ethernet extended with Time-Sensitive Networking technology provides the features required in the area of industrial communication networks, such as:

- Meeting low latency and latency variation requirements concerning data transmission.
- Efficient exchange of data records on a frequent time period.
- Reliable communications with calculable downtime.
- High availability meeting application requirements.
- Efficient mechanisms for bandwidth utilization of exchanges of data records, with zero congestion loss.
- Improved clock synchronization mechanisms, including support of multiple gPTP domains.

Time-sensitive networking profile for industrial automation

1 Scope

This document defines a time-sensitive networking profile for industrial automation. The profile selects features, options, configurations, defaults, protocols, and procedures of bridges, end stations, and LANs to build industrial automation networks.

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9594-1:2020 (ITU-T Recommendation X.500), *Information technology: Open systems interconnection – Part 1: The Directory: Overview of concepts, models and services*

ISO/IEC 9594-2:2020 (ITU-T Recommendation X.501), *Information technology: Open systems interconnection Part 2: The Directory: Models*

ITU-T Recommendation G.781.1, *Synchronization layer functions for packet-based synchronization*

ITU-T Recommendation G.810, *Definitions and terminology for synchronization networks*

ITU-T Recommendation G.8260, *Definitions and terminology for synchronization in packet networks*

IEEE Draft Std P1588e¹ (Draft 0.2, March 2022), *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Amendment: MIB and YANG Data Models*

IEEE Std 802c-2017², *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 2: Local Medium Access Control (MAC) Address Usage*

IEEE Std 802.1AB-2016, *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery*

IEEE Std 802.1ABcu-2021, *IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery Amendment 1: YANG Data Model*

IEEE Std 802.1AC-2016, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Service Definition*

IEEE Std 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identity*

IEEE Std 802.1AS-2020, *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications*

IEEE Draft Std P802.1ASdm (Draft 0.5, January 2022), *IEEE Standard for Local and Metropolitan Area Networks: Timing and Synchronization for Time-Sensitive Applications Amendment: Hot Standby*

¹ Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE SA Standards Board at the time this publication went to Sponsor ballot/press. For information about obtaining drafts, contact the IEEE

² The IEEE standards or products referred to in Clause 2 are trademarks of The Institute of Electrical and Electronics Engineers, Incorporated.

- 368 IEEE Std 802.1CB-2017, *IEEE Standard for Local and Metropolitan Area Networks: Frame*
369 *Replication and Elimination for Reliability*
- 370 IEEE Std 802.1CS-2020, *IEEE Standard for Local and Metropolitan Area Networks: Link-local*
371 *Registration Protocol*
- 372 IEEE Std 802.1CBcv-2021, *IEEE Standard for Local and Metropolitan Area Networks: Frame*
373 *Replication and Elimination for Reliability — Amendment 1: Information Model, YANG Data*
374 *Model and Management Information Base Module*
- 375 IEEE Std 802.1Q-2018, *IEEE Standard for Local and Metropolitan Area Network: Bridges and*
376 *Bridged Networks*
- 377 IEEE Std 802.1Qcc-2018, *IEEE Standard for Local and Metropolitan Area Networks: Bridges*
378 *and Bridged Networks Amendment 31: Stream Reservation Protocol (SRP) Enhancements and*
379 *Performance Improvements*
- 380 IEEE Std 802.1Qcp-2018, *IEEE Standard for Local and Metropolitan Area Networks: Bridges*
381 *and Bridged Networks Amendment 30: YANG Data Model*
- 382 IEEE Draft Std P802.1Qcw (Draft 1.3, February 2021), *Draft Standard for Local and*
383 *Metropolitan Area Networks: Bridges and Bridged Networks, Amendment: YANG Data Models*
384 *for Scheduled Traffic, Frame Preemption, and Per-Stream Filtering and Policing*
- 385 IEEE Draft Std P802.1Qdj (Draft 0.3, June 2022), *Draft Standard for Local and Metropolitan*
386 *Area Networks: Bridges and Bridged Networks, Amendment: Configuration Enhancements for*
387 *Time-Sensitive Networking*
- 388 IEEE Std 802.3-2022, *IEEE Standard for Ethernet*
- 389 IEEE Draft Std P802.3de (Draft 3.0, March 2022), *Draft Standard for Ethernet Amendment 6:*
390 *Enhancements to MAC Merge and Time Synchronization Service Interface for Point-to-Point 10*
391 *Mb/s Single-Pair Ethernet*
- 392 IETF RFC 2986, Nystrom, M. and Kaliski, B., *PKCS #10: Certification Request Syntax*
393 *Specification Version 1.7*, November 2000, available at <https://www.rfc-editor.org/info/rfc2986>
- 394 IETF RFC 5246, Dierks, T. and Rescorla, E., *The Transport Layer Security (TLS) Protocol*,
395 August 2008, available at <https://www.rfc-editor.org/info/rfc5246>
- 396 IETF RFC 5280, Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W.,
397 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)*
398 *Profile*, May 2008, available at <https://www.rfc-editor.org/info/rfc5280>
- 399 IETF RFC 5652, Housley, R., *Cryptographic Message Syntax (CMS)*, September 2009,
400 available at <https://www.rfc-editor.org/info/rfc5652>
- 401 IETF RFC 6020, Bjorklund, M., *YANG: A Data Modeling Language for the Network Configuration*
402 *Protocol (NETCONF)*, October 2010, available at <https://www.rfc-editor.org/info/rfc6020>
- 403 IETF RFC 6022, Scott, M. and Bjorklund, M., *Transport Layer Security (TLS) Extensions:*
404 *Extension Definitions*, January 2011, available at <https://www.rfc-editor.org/info/rfc6022>
- 405 IETF RFC 6066, Eastlake, D., *YANG Module for NETCONF Monitoring*, October 2010, available
406 at <https://www.rfc-editor.org/info/rfc6066>
- 407 IETF RFC 6125, Saint-Andre, P. and Hodges, J., *Representation and Verification of Domain-*
408 *Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX)*
409 *Certificates in the Context of Transport Layer Security (TLS)*, March 2011, available at
410 <https://www.rfc-editor.org/info/rfc6125>
- 411 IETF RFC 6241, Enns, R., Bjorklund, M., Schoenwaelder, J. and Bierman, A., *Network*
412 *Configuration Protocol (NETCONF)*, June 2011, available at [https://www.rfc-](https://www.rfc-editor.org/info/rfc6241)
413 [editor.org/info/rfc6241](https://www.rfc-editor.org/info/rfc6241)

- 414 IETF RFC 6470, Bierman, A., *Network Configuration Protocol (NETCONF) Base Notifications*,
415 February 2012, available at <https://www.rfc-editor.org/info/rfc6470>
- 416 IETF RFC 6961, Pettersen, Y., *The Transport Layer Security (TLS) Multiple Certificate Status*
417 *Request Extension*, June 2013, available at <https://www.rfc-editor.org/info/rfc6961>
- 418 IETF RFC 7317, Bierman, A. and Bjorklund, M., *A YANG Data Model for System Management*,
419 August 2014, available at <https://www.rfc-editor.org/info/rfc7317>
- 420 IETF RFC 7407, Bjorklund, M., and Schoenwaelder, J., *A YANG Data Model for SNMP*
421 *Configuration*, December 2014, available at <https://www.rfc-editor.org/info/rfc7407>
- 422 IETF RFC 7589, Badra, M., Luchuk, A. and Schoenwaelder, J., *Using the NETCONF Protocol*
423 *over Transport Layer Security (TLS) with Mutual X.509 Authentication*, June 2015, available at
424 <https://www.rfc-editor.org/info/rfc7589>
- 425 IETF RFC 7748, Langley, A., Hamburg, M., and Turner, S., *Elliptic Curves for Security*, January
426 2016, available at <https://www.rfc-editor.org/info/rfc7748>
- 427 IETF RFC 7950, Bjorklund, M., *The YANG 1.1 Data Modeling Language*, August 2016, available
428 at <https://www.rfc-editor.org/info/rfc7950>
- 429 IETF RFC 8341, Bierman, A. and Bjorklund, M., *Network Configuration Access Control Model*,
430 March 2018, available at <https://www.rfc-editor.org/info/rfc8341>
- 431 IETF RFC 8342, Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K. and Wilton, R.,
432 *Network Management Datastore Architecture (NMDA)*, March 2018, available at
433 <https://www.rfc-editor.org/info/rfc8342>
- 434 IETF RFC 8343, Bjorklund, M., *YANG Data Model for Interface Management*, March 2018,
435 available at <https://www.rfc-editor.org/info/rfc8343>
- 436 IETF RFC 8525, Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K. and Wilton, R.,
437 *YANG Library*, March 2019, available at <https://www.rfc-editor.org/info/rfc8525>
- 438 IETF RFC 8640, Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E. and Tripathy, A.,
439 *Dynamic Subscription to YANG Events and Datastores over NETCONF*, September 2019,
440 available at <https://www.rfc-editor.org/info/rfc8640>
- 441 IETF RFC 8641, Clemm, A. and Voit, E., *Subscription to YANG Notifications for Datastore*
442 *Updates*, September 2019, available at <https://www.rfc-editor.org/info/rfc8641>
- 443 IETF RFC 9196, Lengyel, B., Clemm, A. and Claise, B., *YANG Modules Describing Capabilities*
444 *for Systems and Datastore Update Notifications*, February 2022, available at <https://www.rfc-editor.org/rfc/rfc9196.html>
445

446 Editor's note: The „Internet-Draft (I-D)“ will be substituted before IEEE SA ballot and IEC
447 CDV with the IETF RFC numbers, which are not yet known. The reference to the draft will
448 also disappear.

- 449 IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Truststore* (draft-ietf-netconf-trust-
450 anchors-19), Internet Draft, Work in Progress by NETCONF WG, available at
451 <https://datatracker.ietf.org/doc/draft-ietf-netconf-trust-anchors/19/>
- 452 IETF RFC „Internet-Draft (I-D)“, *A YANG Data Model for a Keystore* (draft-ietf-netconf-keystore-
453 26), Internet Draft, Work in Progress by NETCONF WG, available at
454 <https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/26/>
- 455 IETF RFC „Internet-Draft (I-D)“, *YANG Data Types and Groupings for Cryptography* (draft-ietf-
456 netconf-crypto-types-25), Internet Draft, Work in Progress by NETCONF WG, available at
457 <https://datatracker.ietf.org/doc/draft-ietf-netconf-crypto-types/25/>
- 458 NIST FIPS 186-4, *Digital Signature Standard (DSS)*, July 2013, available at
459 <https://csrc.nist.gov/publications/detail/fips/186/4/final>

Editor's note: Any draft standards will be removed prior to CDV and SA Ballot.

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 General

For the purposes of this document, the terms and definitions given in ITU-T G.781.1, ITU-T G.810, ITU-T G.8260, IEEE Std 802-2014, IEEE Std 802.3-2022, IEEE Std 802.1Q-2018, IEEE Std 802.1AS-2020, and the following apply:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEEE Standard: available at <https://standards.ieee.org/standard/index.html>
- ITU-T recommendation: available at <https://www.itu.int/ITU-T/recommendations/index.aspx>

NOTE Definitions in IEC 60050 can be found in the Electropedia link above.

3.2 List of terms, abbreviated terms and definitions given in various standards

For the purposes of this document, the terms and definitions given in Table 1 apply.

Editor's note: Any standard referenced in the section title but not referenced in the table will be removed prior to CDV and sponsor ballot.

For ease of understanding, the most important terms used within this profile document are listed in Table 1 but the definitions are not repeated.

Table 1 – List of terms

Term	Source
acquiring mode	ITU-T G.781.1
BMCA	IEEE Std 802.1AS-2020
Bridge	IEEE Std 802.1Q-2018
Bridge Port	IEEE Std 802.1Q-2018
CFM	IEEE Std 802.1Q-2018
Clock	IEEE Std 802.1AS-2020
ClockMaster	IEEE Std 802.1AS-2020
ClockSlave	IEEE Std 802.1AS-2020
ClockSource	IEEE Std 802.1AS-2020
ClockTarget	IEEE Std 802.1AS-2020
CNC	IEEE Std 802.1Qcc-2018
constant time error (cTE)	ITU-T G.8260
CQF	IEEE Std 802.1Q-2018
Customer Virtual Local Area Network (C-VLAN) component	IEEE Std 802.1Q-2018
CUC	IEEE Std 802.1Qcc-2018
DLL	IEEE Std 802-2014
DTE	IEEE Std 802.3-2022
dynamic time error (dTE)	ITU-T G.8260
EEE	IEEE Std 802.3-2022
end station	IEEE Std 802-2014
Ethernet	IEEE Std 802.3-2022

Term	Source
FDB	IEEE Std 802.1Q-2018
FID	IEEE Std 802.1Q-2018
fingerprint	IETF RFC 7589
FQTSS	IEEE Std 802.1Q-2018
fractional frequency offset	IEEE Std 802.1AS-2020
frame	IEEE Std 802.1Q-2018
frame preemption	IEEE Std 802.1Q-2018
free-run mode	ITU-T G.781.1
FRER	IEEE Std 802.1CB-2017
gating cycle	IEEE Std 802.1Q-2018
gPTP communication path	IEEE Std 802.1AS-2020
gPTP domain	IEEE Std 802.1AS-2020
Grandmaster Clock	IEEE Std 802.1AS-2020
Grandmaster PTP Instance	IEEE Std 802.1AS-2020
Independent Virtual Local Area Network [VLAN] Learning (IVL)	IEEE Std 802.1Q-2018
ISS	IEEE Std 802.1AC-2016
IST	IEEE Std 802.1Q-2018
jitter	ITU-T G.810
LAN	IEEE Std 802-2014
latency	IEEE Std 802.1Q-2018
Listener	IEEE Std 802.1Q-2018
LLDP	IEEE Std 802.1AB-2016
LLDPDU	IEEE Std 802.1AB-2016
LocalClock	IEEE Std 802.1AS-2020
locked mode	ITU-T G.781.1
logical link	IEEE Std 802-2014
LPI	IEEE Std 802.3-2022
LRP	IEEE P802.1CS
MAC	IEEE Std 802.1Q-2018
maximum absolute relative time error ($\max TE_R $)	ITU-T G.8260
maximum absolute time error ($\max TE $)	ITU-T G.8260
MMRP	IEEE Std 802.1Q-2018
MST	IEEE Std 802.1Q-2018
MVRP	IEEE Std 802.1Q-2018
NETCONF	IETF RFC 6241
PCP	IEEE Std 802.1Q-2018
PDU	IEEE Std 802.1Q-2018
PHY	IEEE Std 802.3-2022
PLS	IEEE Std 802.3-2022
Port	IEEE Std 802.1Q-2018
primary domain	IEEE Draft Std P802.1ASdm
PSFP	IEEE Std 802.1Q-2018

Term	Source
PTP End Instance	IEEE Std 802.1AS-2020
PTP Instance	IEEE Std 802.1AS-2020
PTP Link	IEEE Std 802.1AS-2020
PTP Port	IEEE Std 802.1AS-2020
PTP Relay Instance	IEEE Std 802.1AS-2020
PVID	IEEE Std 802.1Q-2018
redundancy	IEC 60050-192
relative time error (TE_R)	ITU-T G.8260
residence time	IEEE Std 802.1AS-2020
secondary domain	IEEE Draft Std P802.1ASdm
station	IEEE Std 802-2014
stream	IEEE Std 802.1Q-2018
synchronized time	IEEE Std 802.1AS-2020
Talker	IEEE Std 802.1Q-2018
time error	ITU-T G.8260
time-sensitive stream	IEEE Std 802.1Q-2018
traffic class	IEEE Std 802.1Q-2018
TLV	IEEE Std 802.3-2022
Configuration Domain	IEEE P802.1Qdj
UNI	IEEE Std 802.1Qcc-2018
VID	IEEE Std 802.1Q-2018
VLAN	IEEE Std 802.1Q-2018
YANG	IETF RFC 6020

3.3 Terms defined in this document

3.3.1

application clock

clock used by the application to time events

Note 1 to entry: Events can be periodic or aperiodic.

3.3.2

Bridge component

Customer Virtual Local Area Network (C-VLAN) component as defined in IEEE Std 802.1Q-2018

3.3.3

control latency

time delay between the input to a sensor application and the output from an actuator application

Note 1 to entry: For the purposes of this document, control latency does not include latencies in the sensor, actuator, or the physical system above the process interface in Figure 1.

3.3.4

deadline

application defined fixed time reference point that represents a time when data is required by the application

3.3.5

End station component

end station entity as defined in IEEE Std 802-2014

3.3.6

Global Time

synchronized time, derived from a gPTP domain, that is traceable to the PTP timescale

3.3.7

IA-controller

industrial automation function, consisting of a comparing element and a controlling element, that performs a specified control function

Note 1 to entry: An IA-controller exchanges data with several IA-devices or other IA-controllers for the purpose of control of a system.

Note 2 to entry: The primary categories of IA-Controllers are distributed control system (DCS), programmable logic controller (PLC), and programmable automation controller (PAC).

3.3.8

IA-device

industrial automation function, consisting of sensor and/or actuator elements to read and/or write process data

Note 1 to entry: An IA-device exchanges data with an IA-controller or other IA-devices for the purpose of control of a system.

3.3.9

IA-station

material element or assembly of one or more end station components, and zero, one or more bridge components

Note 1 to entry: IA-controllers and IA-devices are industrial automation functions of IA-stations.

Note 2 to entry: An IA-station is often colloquially called an "IA-controller" or "IA-device" based on its primary function, for example, "IA-controller" for an IA-station that includes an IA-controller function and an IA-device function.

3.3.10

imprinting

<security> equipping IA-stations with an LDevID-NETCONF credential as defined in IEEE Std 802.1AR, corresponding trust anchor as defined in IETF RFC 6024, and certificate-to-name mapping instructions as defined in IETF RFC 7589, Clause 7

3.3.11

management entity

IA-station function responsible for configuration of Bridge components, end station components and ports

Note 1 to entry: The management entity interacts with remote management.

3.3.12

network diameter

longest of all the calculated shortest paths between each pair of nodes in the network

Note 1 to entry: The shortest path between 2 nodes is the path between the two nodes that contains the fewest number of logical links.

3.3.13

network provisioning

process of defining a consistent network configuration, which is applied to all stations

3.3.14

nominal frequency

ideal frequency with zero uncertainty

Note 1 to entry: The nominal frequency of the PTP timescale is further explained in IEEE Std 1588-1029, 7.2.1, 7.2.2, and Annex B.

3.3.15

pDelay interval

Tpdelay2pdelay

interval between transmission of two consecutive pDelay request messages

3.3.16**pDelay turnaround time**

TpdelayTurnaround

interval between reception of a pDelay request message and transmission of the consequent pDelay response message

3.3.17**ppm**

μHz/Hz

Note 1 to entry: Ppm refers to a pure multiplicator of 0,000 001 and is used in the context of this document as an SI unit term to allow readable terms conformant to various rules related to expressions.

3.3.18**Sync residence time**

Tresidence

interval between reception of a Sync message and transmission of the consequent Sync message

3.3.19**Sync drift interval**

Tsync2driftTLV

interval between transmission of a Sync message and transmission of the consequent Drift measurement TLV

3.3.20**Sync Interval**

Tsync2sync

interval between transmission of two consecutive Sync messages

3.3.21**Working Clock**

synchronized time derived from a gPTP domain that is traceable to the PTP timescale, or to an ARB timescale that is continuous

Note 1 to entry: In general, the Working Clock time is traceable to an ARB timescale; however, the Working Clock time can be correlated to a recognized timing standard.

3.4 Abbreviated terms and acronyms

Editor's note: This section will be checked and completed prior to CDV and SA ballot.

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ARB	Arbitrary
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BMCA	Best Master Clock Algorithm
CA	Certification Authority
CBC	Cipher Block Chaining
ccA	Conformance Class A
ccB	Conformance Class B
CFM	Connectivity Fault Management
CMS	Cryptographic Message Syntax
CN	Common Name
CNC	Centralized Network Configuration
CQF	Cyclic Queuing and Forwarding

CRL	Certificate Revocation List
CRUDX	Create Read Update Delete eXecute
CSR	Certificate Signing Request
CUC	Centralized User Configuration
C-VLAN	Customer VLAN
DAC	Discretionary Access Control
DER	Distinguished Encoding Rules
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DLL	Data Link Layer
DMAC	Destination MAC Address
DNS	Domain Name Service
DSA	Digital Signature Algorithm
DTE	Data Terminal Equipment
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EE	End Entity
EEE	Energy Efficient Ethernet
FDB	Filtering Database
FID	Filtering Identifier
FQDN	Fully Qualified Domain Name
FQTSS	Forwarding and Queuing Enhancements for time-sensitive streams
FRER	Frame Replication and Elimination for Redundancy
GCM	Galois Counter Mode
gPTP	generalized Precision Time Protocol
HMAC	Keyed-Hashing for Message Authentication Code
HW	HardWare
IA	Industrial automation
IDevID	Initial Device IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ISS	Internal Sublayer Service
IST	Internal Spanning Tree
ITU	International Telecommunication Union
IVL	Independent Virtual Local Area Network Learning
LDevID	Locally significant Device IDentifier
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LPI	Low Power Idle
LRP	Link-local Registration Protocol
MAC	Media Access Control
MD	Media-Dependent

MDI	Media Dependent Interface
MMRP	Multiple MAC Registration Protocol
MST	Multiple Spanning Tree
MVRP	Multiple VLAN Registration Protocol
N/A	Not applicable
NACM	Network configuration Access Control Model
NETCONF	Network Configuration Protocol
NMDA	Network Management Datastore Architecture
NPE	Network Provisioning Entity
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCP	Priority Code Point
PCS	Profile Conformance Statement
PDU	Protocol Data Unit
PE	Path Entity
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PHY	Physical Layer devices
PII	Personally Identifiable Information
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PLS	Physical Signaling Sublayer
ppm	Parts per million
PSFP	Per-Stream Filtering and Policing
PTP	Precision Time Protocol
PVID	Port VLAN Identifier
RBAC	Role-Based Access Control
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RAE	Resource Allocation Entity
SAN	Subject Alternative Name
SHA	Secure Hash Algorithm
STE	Sync Tree Entity
TDE	Topology Discovery Entity
TLS	Transport Layer Security
TLV	Type, Length, Value
TOFU	Trust On First Use
TSN	Time-Sensitive Networking
TSN-IA	Time-Sensitive Networking for Industrial Automation
TTP	Trusted Third Party
UNI	User/Network Interface

URL	Uniform Resource Locator
VID	VLAN Identifier
VLAN	Virtual Local Area Network
YANG	Yet Another Next Generation data modeling language

3.5 Conventions

3.5.1 Principles for (sub) clause selections of referenced documents

Normative statements in Clause 5 are established based upon the following principles:

- This document shall explicitly identify which parts (clauses, subclauses, figures, lists, tables, etc.) of the cited standards apply to this profile.
- The features of any cited standard that are mandatory (identified by shall), optional (identified by may), prohibited (identified by shall not), or not applicable shall be explicitly identified.
- Additional constraints for features of any cited standard shall be identified.

Editor's note: This subclause (3.5.1) is provided for reference only and will be removed prior to CDV and SA ballot.

3.5.2 Convention for capitalizations

Capitalized terms are either based on the rules given in the ISO/IEC Directives Part 2 or emphasize that these terms have a specific meaning throughout this document.

Throughout this document "bridge" can be used instead of "Bridge", except when

- it occurs at the beginning of a sentence or
- it is being used as (or part of) a specific term such as "VLAN Bridge" rather than being used to identify bridges (potentially of any type) in general. If "VLAN Bridge" is meant where only "Bridge" is written, a change to "VLAN Bridge" would be appropriate.

3.5.3 Unit conventions

This document uses

- Gb/s for gigabits per second and
- Mb/s for megabits per second.

3.5.4 Conventions for YANG contents

YANG modules and XML instance data for YANG shown in this document uses the following style:

Text style `higher-layer-if` text style

Contents of a YANG module use the following style:

```
<ieee802-dot1q-bridge xmlns="urn:ietf:params:xml:ns:yang:ieee802-dot1q-bridge">
  <bridges>
    <bridge> <!-- list -->
      <name>functional-unit-x</name>
      ...
    </bridge>
  </bridges>
</ieee802-dot1q-bridge>
```

4 Overview of TSN in industrial automation

4.1 Industrial application operation

Industrial network applications are based on three main types of building blocks, which may be combined in one IA-controller or provided as a combination of an IA-controller and IA-devices interconnected through a suitable communication network.

These basic building blocks are:

- IA-device Sensor subsystems, which provide input signals indicating the value of the parameter or state being monitored, such as temperature, pressure, or discrete input information.
- IA-controller subsystems, which operate on combinations of measurements and external demand settings to develop output requests, such as position corrections in a motion application.
- IA-device Actuator subsystems, which implement output requests that result in physical changes to the process or machine under control, such as a level in a storage tank, the speed of a printing press, or movement of a robot.

NOTE 1 In general, all subsystems have an internal state, based upon initial settings, and derived from execution; therefore, the application inputs are combined with the internal state to develop an updated internal state and associated outputs.

A control loop is formed when the process or machine responds to the actuator output and produces a new measured value at the sensor. The complete loop is shown in Figure 1 where the IA-controllers and IA-devices are connected as end stations in the network.

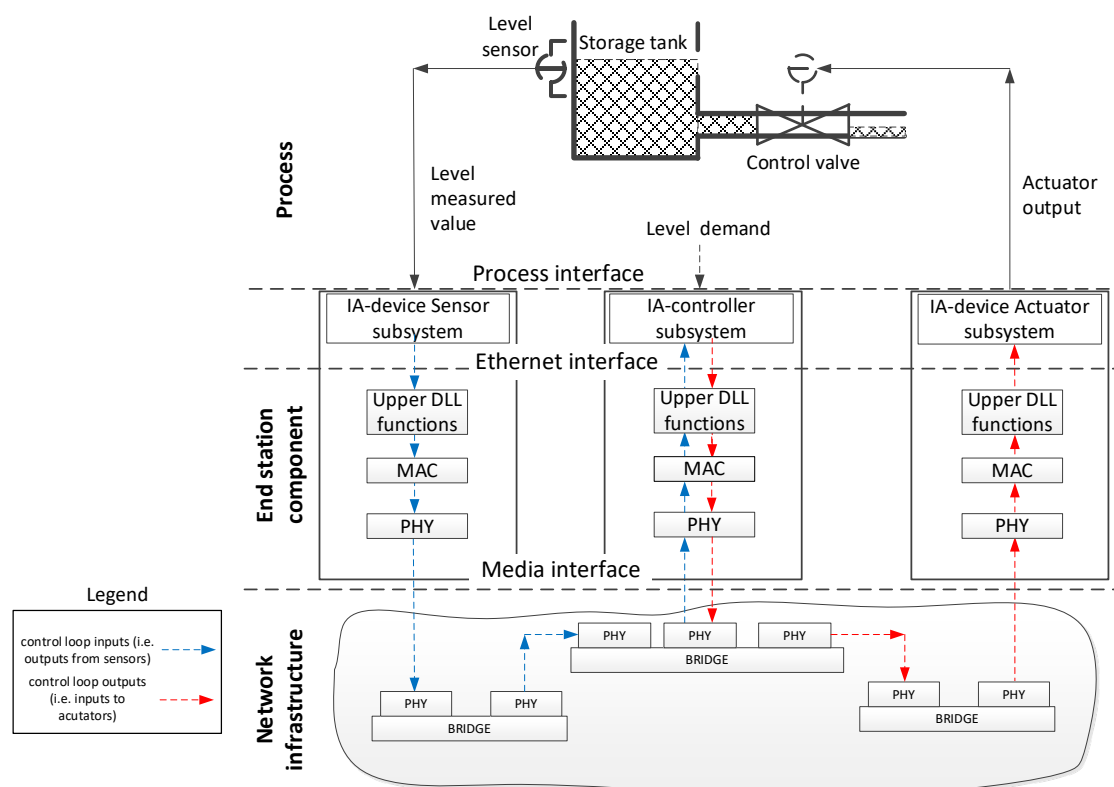


Figure 1 – Data flow in a control loop

In operation, the IA-device Sensor subsystem samples the measured value and the sampled values are transferred through the network as data packets for the IA-controller subsystem to compare with the demand value. After the required computational time, the required output is transferred from the IA-controller subsystem to the IA-device Actuator subsystem for implementation as a change in the external process.

This sequence repeats continuously as a regular operation using a Working Clock. The Working Clock can be traceable to an ARB or PTP timescale, but this traceability is not required by all applications. For stability, the time constant of the process response needs to be on the order of five to ten times (or more) the sequence repetition time (i.e., sampling time).

NOTE 2 In common Industrial Network deployments, it has been observed that a ratio of 5 to 10 (or more) provides effective control of the automated process. The actual ratio of the process response time constant to sampling time required for stability depends on the implementation.

Control latency is a critical factor in all types of control and needs to be bounded.

Components of the control latency time are shown in Figure 1.

- Application time for sampling, computation, and processing within each IA-controller and IA-device. These are specific to the IA-device and IA-controller and known to the IA-device or IA-controller makers.
- The time for data transfer through the upper DL functions, MAC and PHY layers within each IA-controller and IA-device. This time depends on the implementation of these components, their situation-dependent load and performance, and configuration elements related to QoS and TSN that some of these components may support.
- End Station and Bridge scheduling and transfer time through the network. These are influenced by the configuration process, which allocates available bandwidth and priorities to various types of application messages.

Offline engineering of the network is possible, including the calculation of the control latency time. During system operation, management services are provided for diagnostics and checking the performance indicators of an installed network.

4.2 Industrial applications

4.2.1 General

Industrial applications can contain multiple tasks. These tasks are executed based upon time or other events. Thus, an industrial application can have multiple tasks executing on different cycles as shown in Figure 2 and Figure 3.

Examples of these tasks are listed below.

- Background tasks, which are executed when no other task is running. There can be zero, one, or more such tasks in an industrial application.
- Main task which executes periodically. The start and execution of this task is often based upon the ARB timescale. There can be zero or one such task, in an industrial application.
- Global Time tasks. The start and execution of these tasks is often based upon Global Time (for example, at noon every day, at noon every Friday, etc.). There can be zero, one or more such tasks in an industrial application.
- Process driven tasks which are started by an event (for example, a sensor value reaches a defined point, a process fault occurs, etc.). There can be zero, one or more such tasks in an industrial application.
- Control loop tasks which are bound to Working Clock and started periodically. There can be zero, one or more such tasks in an industrial application.

A user defines the required automation tasks along with the data objects required as output and input for these tasks and the end station which hosts these tasks. Thus, these tasks are bound to data objects, which need to be exchanged between end stations per the user's definition. Many of these tasks have timing requirements, which are added as attributes to the assigned data objects. Examples of these attributes include:

- [DataObject_Update_Interval] an update interval (time between two consecutive updates at the transmitting end station);
- [DataObject_Deadline] a deadline (latest receive time at the end station, relative to the start of the DataObject Update Interval);

- [DataObject_Data_Size] the size of the DataObject;
- Other attributes as needed to form a stream-list request according to IEEE Draft P802.1Qdj, 46.1.5.

NOTE These attributes are provided for illustration purposes. The list is not representative of all industrial applications. These are not network attributes.

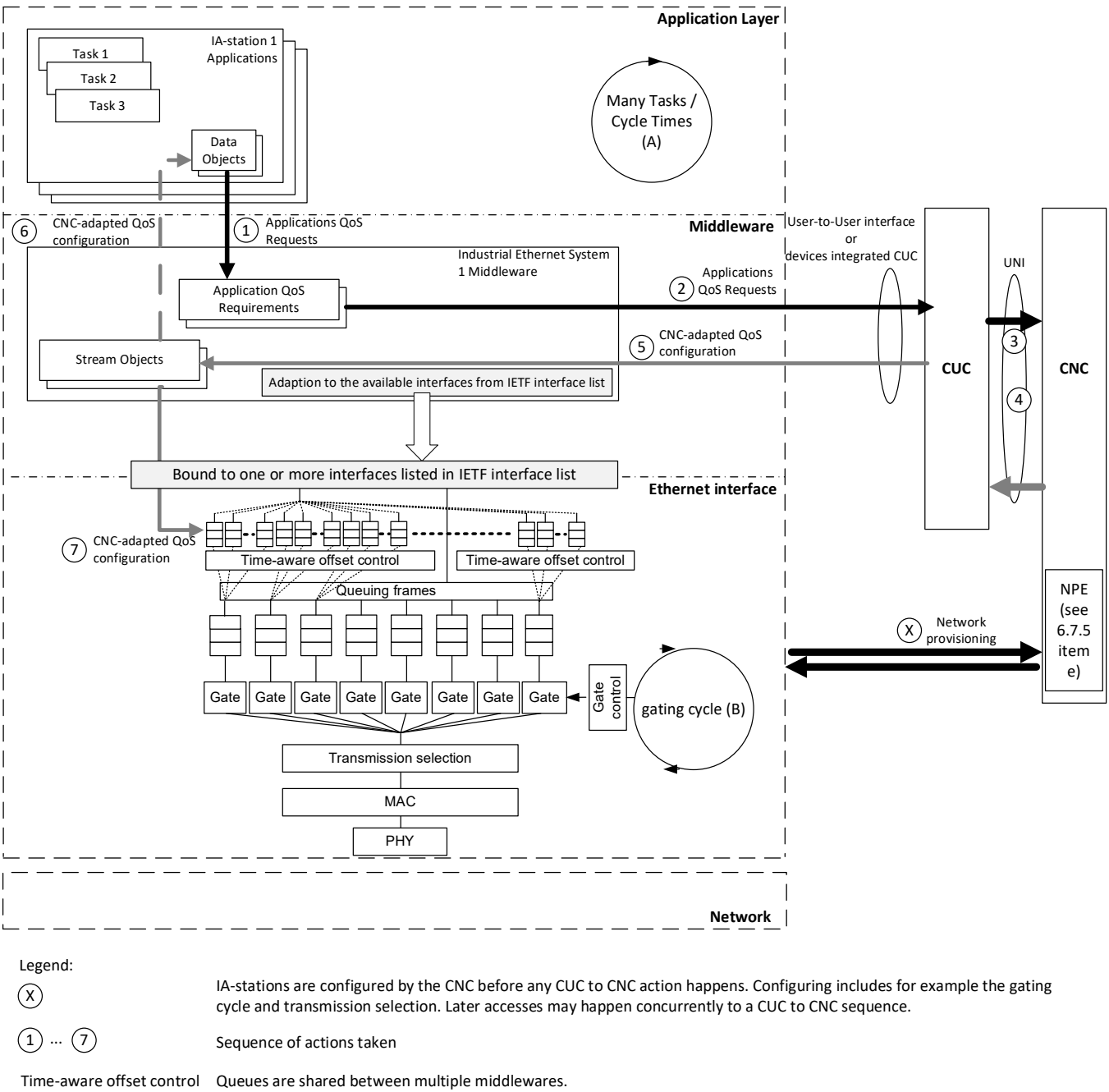


Figure 2 – IA-station interaction with CNC – Transmit path

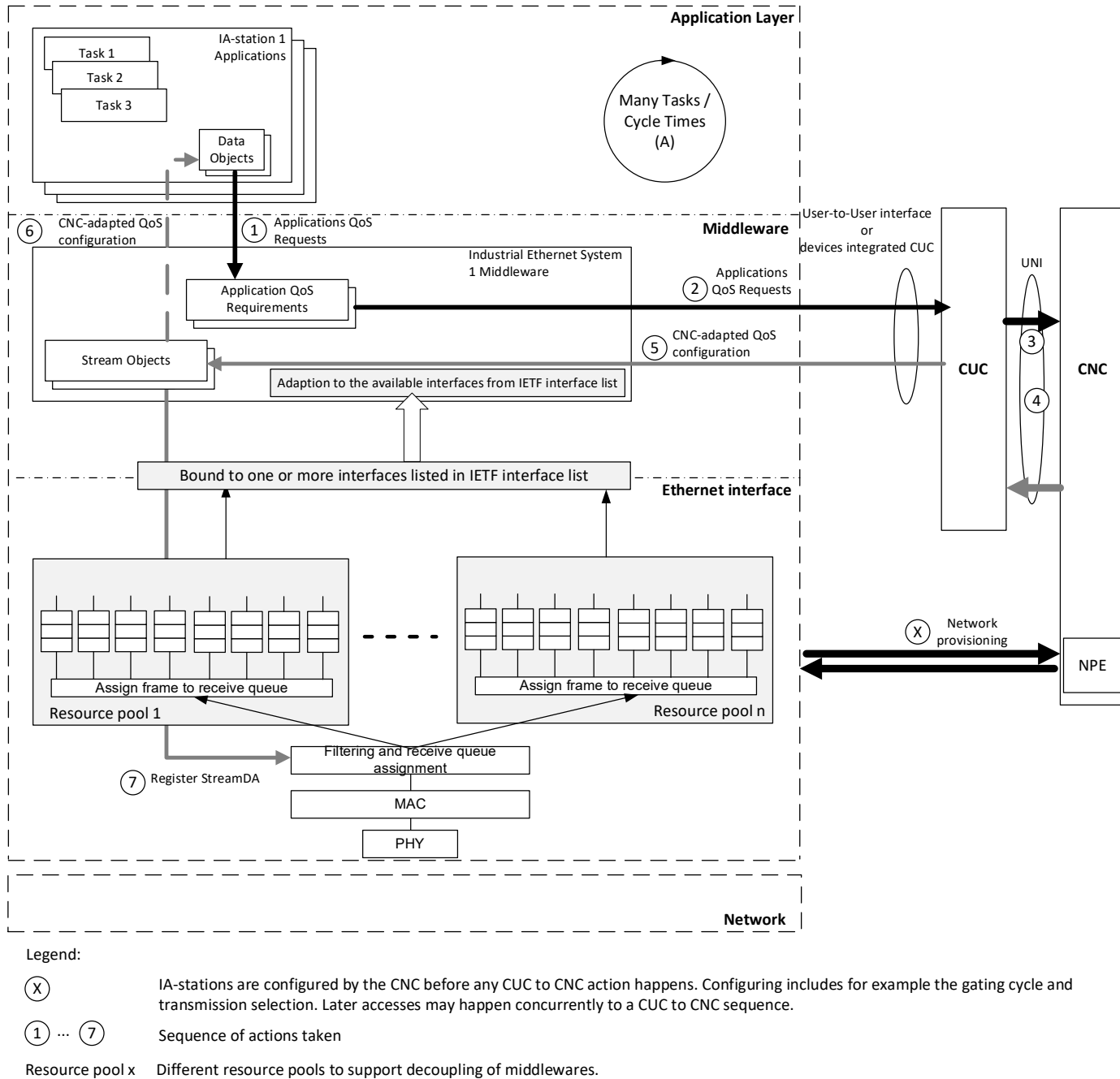


Figure 3 – IA-station interaction with CNC – Receive path

4.2.2 Control loop tasks

Control loops rely on the behavior of synchronized tasks by each of the IA-devices and IA-controllers involved in that control loop. For example, this behavior can be implemented by using a common Working Clock, a common starting point relative to the Working Clock and a common duration for this control loop task at the involved IA-devices and IA-controllers. The data objects associated with the control loop share common values for some attributes (for example, the same values for DataObject_Update_Interval and DataObject_Deadline). Multiple control loop tasks can be implemented and running in parallel at the involved automation devices.

4.2.3 Start of control loop tasks

The calculation of the starting point for a control loop task is independent from the time when the device is powered up or connected to the Configuration Domain. The start of a control loop task, which is based on the Working Clock, can be calculated in the following manner:

Divide the Working Clock value, expressed as an integer, by the duration of the control loop task, expressed as an integer, whenever the Working Clock value increases by one. A remainder of zero provides the basis for the start of the control loop task.

NOTE The units of the Working Clock value and the duration of the control loop task are the same.

Stations in the network associated with the control loop synchronize to a Working Clock using IEEE Std 802.1AS-2020.

4.3 IA-stations

An IA-station can be a simple end station acting as source or destination for control data traffic. In addition, an IA-station can be a combined functional unit that includes an end station component together with a Bridge component in one chassis. IA-stations, incorporating multiple functional units with several end station components and Bridge components within one chassis, can also be found in industrial automation. Within this kind of combined IA-station various components can be connected by internal ports and internal LANs. All components utilize a common management entity as shown in Figure 4.

Figure 4 shows an example IA-station incorporating three functional units in one chassis. Functional unit 1 and functional unit 2 each consist of a Bridge component and an end station component. The end station components are connected by internal ports via internal LANs to the Bridge components. The Bridge components include two external ports each. Functional unit 3 includes only a single end station component with one external port.

IA-controllers and IA-devices as well as the management entity are IA-station functions acting as source of and/or destination for link layer data traffic. Thus, each IA-station incorporates at least one end station component where these functions can be located. Figure 4 shows that IA-station functions can either reside in a single end station component (IA-device 1, IA-controller 1, IA-device 2) or in multiple end station components (IA-controller 2, management entity).

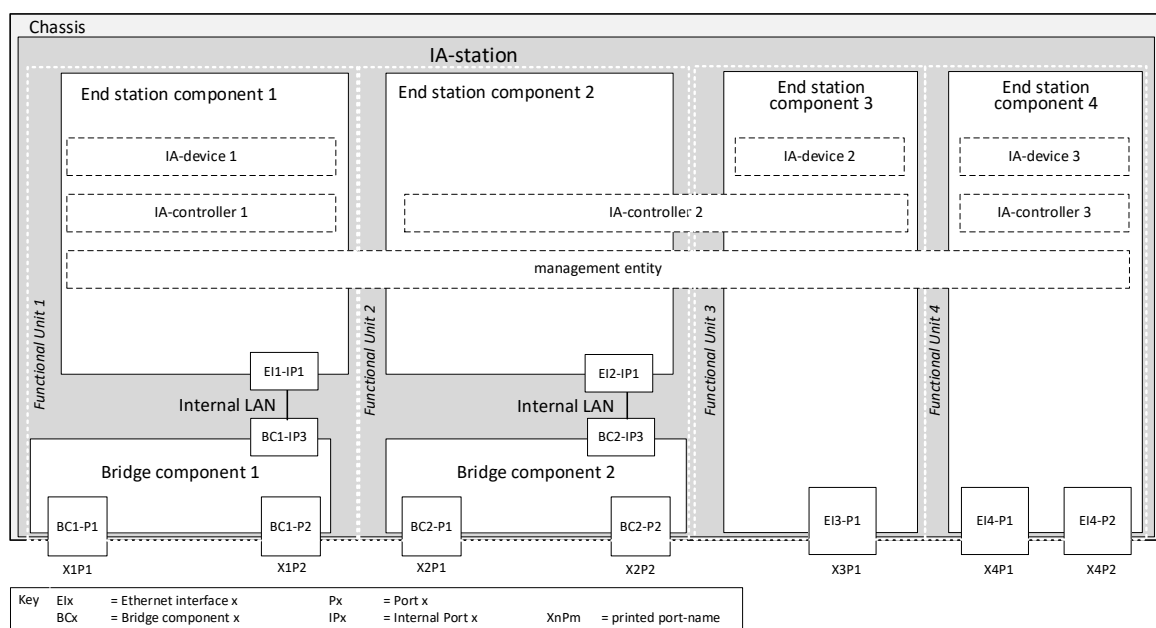


Figure 4 – IA-station example

4.4 Ethernet interface

One or more middleware components act as a layer between applications and the Ethernet interface. Figure 2 and Figure 3 show the relation between applications, middleware, Ethernet interface and the network. Various applications can run in parallel on an automation device.

Data objects represent the information exchanged between applications running in different end stations. The application requirements contained in these data objects are translated by the middleware into stream requirements for use by the CUC. This translation can be accomplished in one of the following ways:

- a) The user defines the data objects and translates them into stream requirements and end-station communication-configurations. A user-specific mechanism is used to configure the network components and establish paths.
- b) The user defines the data objects and associates them with QoS requirements for each stream (application QoS requirements). These can be forwarded as stream requirement requests by a CUC to a CNC. The CNC would respond by providing a stream configuration response. The request and response are specified in IEEE P802.1Qdj. The CUC can be integrated into the end station or can be accessed via a user-to-user protocol. The middleware uses this information for configuring Talkers and Listeners. This information is also used to add additional timing information to the data objects for application usage.
- c) Time-aware offset control utilizes per-stream queues (see IEEE Std 802.1Q-2018, figure 34-1) and the traffic specification of the streams, including transmission offsets, provided by the CNC to ensure the order of stream transmission.

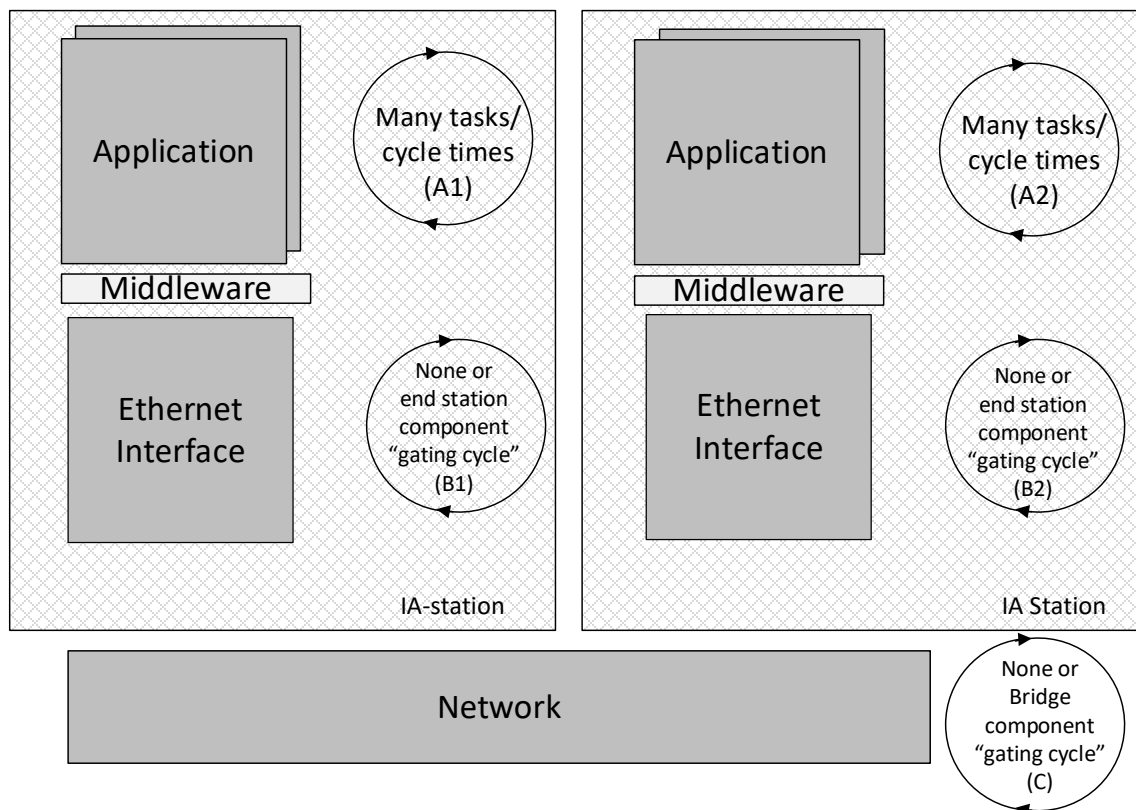


Figure 5 – Model for cycles

These automation systems, which are built from various end stations and connected via bridges, can share a common gating cycle or each station can have its own gating cycle. Alternatively, a bridge or end station can have no gating cycle (expressed as "none" in Figure 5).

4.5 Mechanisms that can be used to meet control loop latency requirements

Meeting latency requirements on a network can be accomplished using one or more combinations of the mechanisms enumerated below. The choice of a mechanism or a subset of the mechanisms listed below depends on the nature of the application(s) and the corresponding latency requirements:

- a) Defining, testing, and simulating all possible application combinations and associated traffic patterns
- b) Overprovisioning the network
- c) Providing scheduled time slots for each application to transmit on the network
- d) Preempting lower priority traffic
- e) Providing scheduled time slots for certain traffic classes
- f) Time-aware offset control
- g) Enforcing deterministic queuing delays in bridges

NOTE This list is not comprehensive and not all mechanisms mentioned here are part of this specification. For specific mechanisms covered by this document please refer to Clause 5.

Frame preemption is specified in IEEE Std 802.1Q-2018 and IEEE Std 802.3-2022.

Reserving time on the network for certain traffic types can be done through enhancements for scheduled traffic according to IEEE Std 802.1Q-2018, 8.6.8.4. An aligned gating cycle needs to be defined for this method to work. Once these aligned gating cycle times are defined, portions of that cycle time can either be allocated to streams or classes of streams.

Multiple Talker/Listener(s) pairs can be used for streams between end stations. Engineered time triggered transmit can be used to coordinate transmission of all the traffic that shares a network to keep application requirements.

Creating a traffic load model in advance will allow analysis of resulting traffic. It can be used to select and implement appropriate mechanisms to achieve latency requirements.

4.6 Translation between middleware and network provisioning

4.6.1 Interfaces of type I2vlan

Application engineering can be done without knowledge of the network provisioning. Thus, application engineering is not able to align the use of, for example, PCP or VID with network provisioning. This problem is solved by providing a translation table (by a YANG module definition for example) to the middleware. The IA-station's local YANG database will store this information.

Figure 6 and Figure 7 show examples of the translation models.

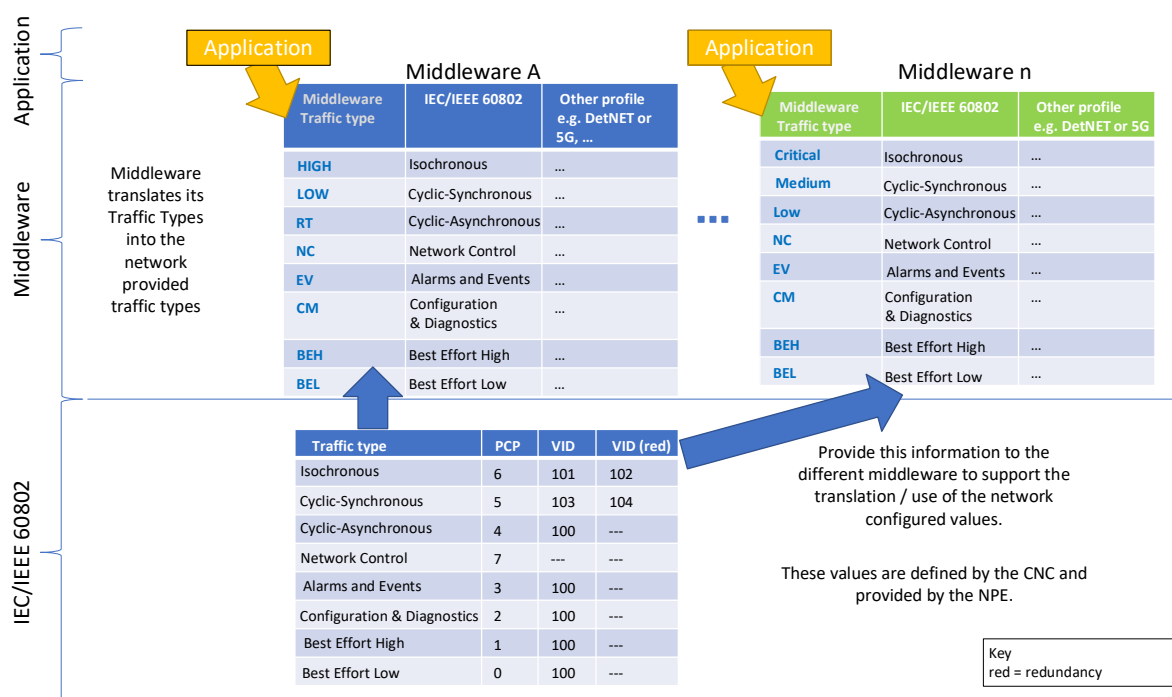


Figure 6 – Traffic type translation example

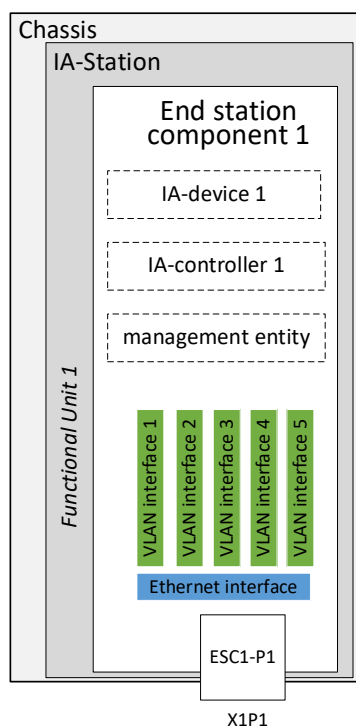


Figure 7 – IETF Interfaces used for Traffic Type Translation

Interfaces of type I2vlan can be used to provide the required mapping information to all installed middleware and applications.

The name string of the I2vlan interfaces can provide the vlan-id, the assigned traffic types with their PCP values and redundancy information (see 6.7.2.3).

4.6.2 PTP Instances

Another item of information which is configured during network provisioning is the PTP domain number. The middleware needs to know which PTP domain is assigned to which target clock. This is done by providing well-defined descriptionDS.userDescription names according to IEEE Std 1588-2019, 8.2.5.5 in order to create a translation table.

Editor's note: descriptionDS.userDescription is not currently part of the IEEE Std 802.1AS-2020. It is expected that it will be incorporated as part of IEEE P802.1ASdm. It may be necessary to update the reference at that time.

descriptionDS.userDescription names allow the support of multiple middlewares at one IA-station using the same PTP Instances (see 6.2.12). Station's local database would store this information.

Figure 8 and Figure 9 show examples of the translation models.

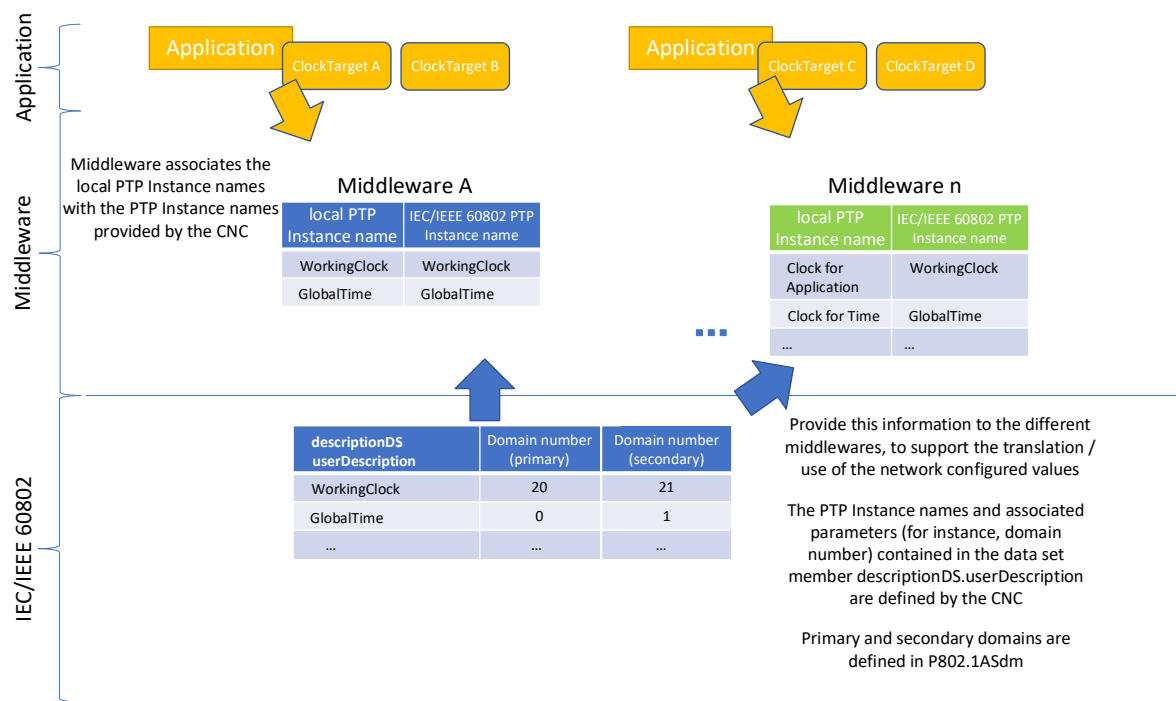


Figure 8 – PTP Instance Translation Example

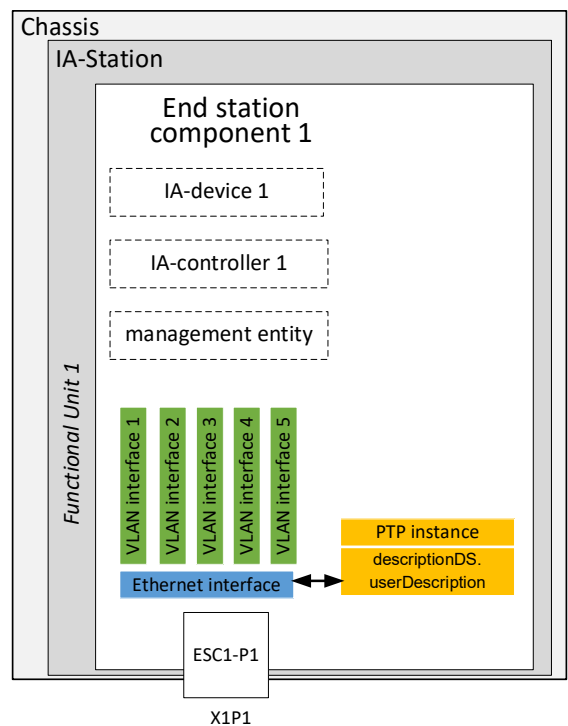


Figure 9 – IETF Interfaces used for PTP Instance Translation

The userDescription contains the clock type (i.e., WorkingClock, GlobalTime, or both) and the attached Ethernet interfaces.

This information is used by the middleware to align to the intended ClockTarget or ClockSource.

4.7 Industrial traffic types

4.7.1 General

Industrial automation applications make use of different traffic schemes/types for different functionalities (for example, parameterization, control, alarming). The various traffic patterns have different characteristics and thus, impose different requirements on a network. To specify these traffic types, a two-step approach is used:

- a) First define characteristics of generic traffic types (traffic-type-categories) and
- b) Second define instances of the generic types, i.e. the traffic types.

4.7.2 Traffic type characteristics

The traffic type characteristics in Table 2 enable the identification of several distinct traffic types that are shared among sets of industrial applications.

Table 2 – Traffic type characteristics

Characteristic	Description
Cyclic	Traffic types consist of frames that can either be transmitted on a reoccurring time period (cyclic) or at no set period (acyclic). Available selections are: - Required: cyclic - Optional: Implementation of cyclic traffic is at the discretion of the user.
Data delivery requirements	Denotes the delivery constraints for the traffic. Four options are specified: - Frame Latency: data delivery of a frame for a given Talker-Listener pair occurs within a bounded timespan. - Flow Latency: data delivery up to a certain number of frames or data size (including bursts of frames) occurring over a defined period. - Deadline: data delivery of a frame to a given Listener occurs at or before a specific point in time. - No: Denotes the case of traffic types with no special data delivery requirements
Time-triggered transmission	Talker data transmission occurs at a specific point in time based upon the Working Clock. Available selections are: - Required - Optional: Implementation of time-triggered transmission is at the discretion of the user. Enhancements of scheduled traffic is only one means of achieving time-triggered transmission. Other, application-based, methods are possible

4.7.3 Traffic type categories

4.7.3.1 General

This two-step approach allows a clear differentiation between characteristics as seen from the “network” point of view and “application” point of view. Traffic-type-categories allow different IEEE 802 feature selections to achieve the specified goals. Four traffic-type-categories are identified in Industrial Automation (IA) systems:

- a) IA time-aware stream
- b) IA stream
- c) IA traffic engineered non-stream
- d) IA non-stream

4.7.3.2 IA time-aware stream

The characteristics of this traffic are shown in Table 3.

Table 3 – IA time-aware stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Deadline or Frame Latency
Time-triggered transmission	Required

4.7.3.3 IA stream

The characteristics of this traffic are shown in Table 4.

Table 4 – IA stream characteristics

Characteristics	
Cyclic	Required
Data delivery requirement	Frame Latency
Time-triggered transmission	Optional

4.7.3.4 IA traffic engineered non-stream

The characteristics of this traffic are shown in Table 5.

Table 5 – IA traffic engineered non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	Flow Latency
Time-triggered transmission	Optional

4.7.3.5 IA non-stream

The characteristics of this traffic are shown in Table 6.

Table 6 – IA non-stream characteristics

Characteristics	
Cyclic	Optional
Data delivery requirement	No
Time-triggered transmission	Optional

4.7.4 Traffic types**4.7.4.1 General**

Table 7 summarizes relevant industrial automation traffic types and their associated characteristics. In an industrial automation system, other applications, such as audio or video, would utilize one of these traffic types. Traffic Type codes are needed for the VLAN naming scheme defined in this document. See 6.7.2.4 for more information.

Table 7 – Industrial automation traffic types summary

Traffic type name	Traffic type code	Cyclic	Data delivery requirements	Time-triggered transmission	Traffic-type-category
Isochronous	H	Required	Deadline	Required	IA time-aware-stream
Cyclic-synchronous	G	Required	Frame Latency	Required	IA time-aware-stream

Traffic type name	Traffic type code	Cyclic	Data delivery requirements	Time-triggered transmission	Traffic-type-category
Cyclic-asynchronous	F	Required	Frame Latency	Optional	IA stream
Alarms & Events	E	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Configuration & Diagnostics	D	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Network Control	C	Optional	Flow Latency	Optional	IA traffic engineered non-stream
Best Effort High	B	Optional	No	Optional	IA non-stream
Best Effort Low	A	Optional	No	Optional	IA non-stream

892

893 4.7.4.2 Isochronous

894 A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-
895 triggered transmission. Listeners have individual deadline requirements. Cycle times are
896 typically in the range of microseconds to tens of milliseconds. Frame size is typically below 500
897 octets. Talker-Listener pairs are synchronized to the Working Clock. The network is configured
898 by the CNC to provide zero congestion loss for this traffic type. This type of traffic is normally
899 used in control loop tasks.

900 4.7.4.3 Cyclic-synchronous

901 A type of IA time-aware stream traffic. This type of traffic is transmitted cyclically using time-
902 triggered transmission. Talker-Listener pairs have individual latency requirements. Cycle times
903 are typically in the range of hundreds of microseconds to hundreds of milliseconds. Frame size
904 is unconstrained except as indicated in 5.5.1. Talker-Listener pairs are synchronized to the
905 Working Clock. The network is configured by the CNC to provide zero congestion loss for this
906 traffic type. This type of traffic is normally used in control loop tasks.

907 4.7.4.4 Cyclic-asynchronous

908 A type of IA stream traffic. This type of traffic is transmitted cyclically with latency requirements
909 bounded by the interval as defined in IEEE Std 802.1Qcc-2018, 46.2.3.5.1. Talker-Listeners
910 pair have individual latency requirements. Cycle times are typically in the range of milliseconds
911 to seconds. Frame size is unconstrained except as indicated in 5.5.1. Data exchanges between
912 Talker-Listener pairs are typically not dependent on the Working Clock. This traffic type typically
913 tolerates limited congestion loss. The network is configured by the CNC to handle this traffic
914 type without loss, up to a certain number of frames or data size.

915 4.7.4.5 Alarms and events

916 A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or
917 acyclically. This traffic expects bounded latency including time for retransmission in the range
918 of milliseconds to hundreds of milliseconds. The source of the alarm or event typically limits the
919 bandwidth allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1.
920 Congestion loss can occur. Retransmission to mitigate frame loss is expected. The network is
921 configured by the CNC to handle these frames, including bursts of frames, up to a certain
922 number of frames or data size over a defined period.

923 4.7.4.6 Configuration and diagnostics

924 A type of IA traffic engineered non-stream. This type of traffic is transmitted cyclically or
925 acyclically. This traffic expects bounded latency, up to seconds, including time for
926 retransmission. The source of configuration or diagnostics frames typically limits the bandwidth
927 allocated to this traffic. Frame size is unconstrained except as indicated in 5.5.1. Congestion
928 loss can occur. Retransmission to mitigate frame loss is expected. The network is configured
929 by the CNC to handle these frames, including bursts of frames, up to a certain number of frames
930 or data size over a defined period.

4.7.4.7 Network control

A type of IA traffic engineered non-stream. This type of traffic can be transmitted cyclically or acyclically. This traffic expects bounded latency including time for retransmission. Frame size is unconstrained except as indicated in 5.5.1. The network is configured by the CNC to handle these frames, including bursts of frames, up to a certain number of frames or data size over a defined period. If these limits are exceeded congestion loss may occur. Network control is comprised of services required to maintain network operation. Examples include time synchronization, loop prevention, and topology detection.

4.7.4.8 Best effort

A type of IA non-stream. The network is configured by the CNC to ensure that these frames do not interfere with other traffic types. These frames are forwarded when resources are available. Congestion loss can occur; therefore, frames may be dropped. It is sometimes desirable to have more than one traffic class for best effort traffic (see Table 8)

4.7.4.9 Traffic class to traffic type mapping

Table 8 provides an example for the usage of traffic classes based on the traffic type:

Table 8 – Example traffic class to traffic type mapping

Traffic class	PCP	Traffic Type
7	6	Isochronous
6	5	Cyclic-Synchronous
5	4	Cyclic-Asynchronous
4	7	Network Control
3	3	Alarms and Events
2	2	Configuration & Diagnostics
1	1	Best Effort High
0	0	Best Effort Low

NOTE 1 The example in Table 8 assumes an implementation supporting eight queues.

NOTE 2 An example mapping of PCP and traffic type to an application is provided in Figure 6.

The traffic-type-categories definition allows different IEEE 802 feature selections to achieve specified goals. Moreover it helps in identification of the traffic protection mechanisms. Adherence to this example of a common mapping helps minimize potential conflicts between traffic types.

4.8 Security for TSN-IA

4.8.1 General

Subclause 4.8 describes selected aspects of TSN-IA security in an informative way. Protecting the management of industrial communication is the main objective of TSN-IA security. The protection of communications that use industrial traffic types is left to an individual middleware and/or application that uses TSN-IA.

4.8.2 Security configuration model

Security configuration is a part of system engineering and configuration. The security configuration in this document does not encompass the supply of configuration objects for middleware and application security. Security configuration settles the prerequisites for protecting the establishment and management of communications that use industrial traffic types (see 4.7). It ensures that the security features of IA-stations (including CNCs) can be used for protecting message exchanges and authorizing the resource accesses during stream

establishment and management. This security configuration supplies deployment-specific configuration objects to IA-stations. They encompass:

- Instructions about cryptographic algorithms
- Credentials and trust anchors
- Instructions to interpret the outcome of peer entity authentication in course of enforcing resource access controls
- Access control rules and permissions

This security configuration uses NETCONF/YANG request/response exchanges:

- The to-be-configured IA-stations act in NETCONF server role with respect to their security configuration.
- A NETCONF client is responsible for setting-up IA-stations for security. This NETCONF client possesses information about the security relationship to be established during security configuration or about the expectations on the IA-stations in a domain. It can be implemented as part of an interactive component (for example, engineering tool) or an automated component (for example, CNC). As an implication, the security configuration includes options for interactive and automated setup, i.e., security configuration is done by human and/or non-human actors.

NOTE NETCONF notifications can also be used to recognize events such as a near-term end-of-life of certificate objects, especially EE certificate objects.

- The security configuration exchanges supply deployment-specific objects (trust anchors, credentials etc.) to IA-stations and manage them. This is security critical. IA-stations that are in factory default state can only possess manufacturer-specific security objects (trust anchors, credentials etc.) when booting initially. The protected NETCONF/YANG exchanges with IA-stations that are in factory default state are outlined in 4.8.3 to 4.8.6.

4.8.3 NETCONF/YANG processing

Securing NETCONF/YANG resources on NETCONF servers is mandated by IETF RFC 6241 (NETCONF). This demands message exchange protection between NETCONF clients and servers as well as resource access authorization by NETCONF servers:

- IETF RFC 7589 (NETCONF-over-TLS) specifies a solution to protect NETCONF message exchanges by TLS.
- IETF RFC 8341 (NACM) specifies three access control points, covering the request/response and notification model in NETCONF according to IETF RFC 8341, 2.1.

NETCONF servers enforce the mandated security as shown in Figure 10. The processing steps are executed upon the current configuration of the NETCONF server's YANG modules.

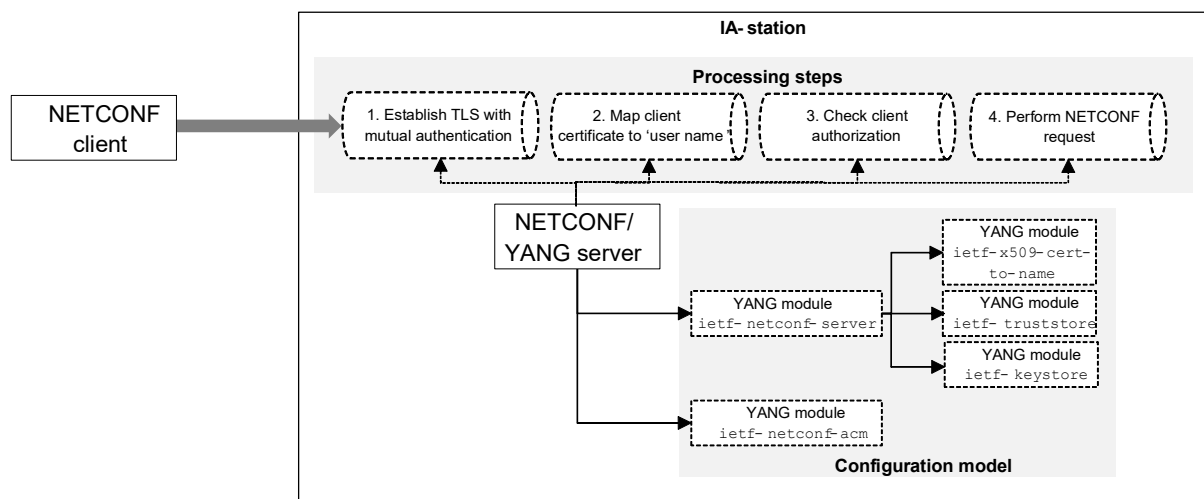


Figure 10 – NETCONF/YANG security processing steps

The processing steps on the side of NETCONF servers are:

- 1) Establish a TLS connection with mutual authentication: The NETCONF server acts as TLS server and awaits connection requests of NETCONF clients (TLS clients). During the TLS handshake the NETCONF server authenticates itself towards the NETCONF client by a credential from its ietf-keystore YANG module. In addition, the NETCONF server challenges the NETCONF client for authentication and verifies its authentication by trust anchors in its ietf-truststore YANG module according to 6.3.4. A successful mutual authentication is a prerequisite for proceeding to the next step.
- 2) Map the client certificate to a username: The NETCONF server maps the authenticated TLS client certificate to a “NETCONF username”³ by applying an ordered list of mapping instructions. These instructions are provided in its ietf-x509-cert-to-name YANG module. The applicable list item is identified by matching its configured fingerprint (according to IETF RFC 7589, Clause 7) against the certification path that was used for TLS client authentication (an end entity certificate or a CA certificate). According to the map type of the identified list item, the NETCONF server determines the “NETCONF username”. This can be done by extracting information from the end entity certificate of the NETCONF client. A successful certificate-to-“NETCONF username” mapping is a prerequisite for proceeding to the next step.
- 3) Check client authorization: The NETCONF server checks if the NETCONF client has the permission to access the requested NETCONF/YANG resource based on its “NETCONF username” and the access control rules available in its ietf-netconf-acm YANG module. See 4.8.4 for more information about NETCONF/YANG access control. A successful authorization is a prerequisite for proceeding to the next step.
- 4) Perform NETCONF request: If all preceding steps succeeded, the NETCONF server performs the NETCONF request.

4.8.4 NETCONF/YANG access control

NACM defines a YANG information model for describing permitted/denied access operations. NETCONF servers are responsible to enforce access control to their resources according to the information in their ietf-netconf-acm YANG modules. In the conceptual dimension of resources, NACM allows the description of access controlled resources in terms of NETCONF protocol operations, nodes in YANG datastores and/or types of notification events. In the conceptual dimension of subjects, NACM uses character strings to represent the subject actors i.e., NETCONF clients. These character strings are known as “NETCONF username”. The NACM access control information of a NETCONF server needs to be created, updated, and deleted per IA-station. The management of this information needs to happen along the IA-

³ In this document, 'NETCONF username' values do not present references to human users – in almost all cases.

station lifecycle for example, manufacturing, bootstrapping, operation, maintaining, re-owning, destructing. Moreover, the management of the NACM access control information itself is subject to NACM access control.

This document employs multiple YANG information models for fulfilling its purposes. This extends beyond the above identified YANG modules (see 4.8.3). The NETCONF server on an IA-station needs to enforce access control for NETCONF/YANG resources. To meet this objective the NETCONF server on an IA-station needs to be supplied with access control information for the used NETCONF/YANG resources. NACM is employed for this purpose and profiles default access control information for the NETCONF/YANG resources (see 6.3.2.2). This relieves other organizations or individuals for example, manufacturers, integrators, operators, owners from being responsible to create NACM access control information for the respective NETCONF/YANG resources.

With respect to the conceptual dimension of subjects, a dedicated profiling strategy is needed to meet the constraints that are given by NACM:

- NACM relies on character strings (known as “NETCONF username”) to refer to clients.
- The actual names of individual entities in organizations are not known while writing this document.

NACM access control information as specified in this document, populates the “NETCONF username” character strings in NACM with role names specified in 6.3.2.1.4, c). This allows to create default NACM information without knowing actual names of individual entities. A role name can refer to 0, 1 or more individual entities. It is the responsibility of users to assign role names to individual entities. This happens by binding the assigned role names to the credentials of individual entities. The current form to express this binding is a role extension in the identity certificates of end entities defined in this document. These are NETCONF clients, i.e., these role extensions appear in the end entity certificates of LDevID credentials for NETCONF clients.

4.8.5 Identity checking

IETF RFC 7589 (NETCONF-over-TLS) requires NETCONF clients to check the identity of NETCONF servers as well as NETCONF servers to check the identity of NETCONF clients.

The NETCONF server identity check happens inside NETCONF clients. It matches an actual against an expectation:

- The actual server identity is established by the end entity certificate of the NETCONF server (authenticated by means of TLS).
- The expectations on server identity are established by the information that is used to connect to the NETCONF server.

IETF RFC 7589 refers to IETF RFC 6125 for the details of retrieving the actual and comparing it against expected.

The NETCONF client identity check happens inside NETCONF servers. It also matches an actual against an expectation:

- The actual client identity is established by the end entity certificate of the NETCONF client (authenticated by means of TLS).
- The expectations on client identity are established by the contents of the YANG modules ietf-netconf-acm and ietf-x509-cert-to-name.

The details of this check are subject to the requested NETCONF operation. IETF RFC 7589, Clause 7, specifies the mapping of an authenticated client certificate to a “NETCONF username” whose permissions are then enforced by IETF RFC 8341 (NACM). More information is provided in 4.8.3, steps 2 and 3.

4.8.6 Secure device identity

4.8.6.1 Device Identity

The term 'device' originates from IEEE Std 802.1AR. It matches the term IA-station in this document.

The device identity refers to a set of information items about a device respectively an IA-station that:

- describes a device as a physical or virtual entity in a distributed system (identifier and/or attribute information)
- is used by a device to describe itself as such entity (identifier and/or attribute information)
- allows to interact with this device (addressing information i.e., a specific identifier class).

The targeted use case, for example application data exchanges, configuration exchanges, inventory, or ordering, determines the required amount of identity information about a device respectively an IA-station.

The device identity of any single IA-station encompasses:

- MAC addresses, IP addresses, TCP ports, DNS names
- ietf-hardware YANG module contents (IETF RFC 8348)

4.8.6.2 Verifiable Device Identity

Certain aspects of device identity demand verification before relying on them during online interactions. These are examples.

- DNS names or IP addresses are used to call the management entity of an IA-station i.e., its NETCONF/YANG server. Their value represents the caller's expectation on the identity of their responder in network communications. Its verification allows to defeat DNS spoofing, component impersonation and man-in-the-middle attacks. This is mandated by IETF RFC 7589 and described in IETF RFC 6125. Passing this check is a prerequisite before NETCONF application exchanges can happen.
- mfg-name values in instances of the ietf-hardware YANG module. These values make claims about the IA-station manufacturer. Their verification is a means to protect against counterfeiting.

The verification of IA-station identity happens according to a model that is fully specified by this document and whose checking can be done in a manufacturer-agnostic manner. This verification is important before supplying locally significant credentials especially LDevID-NETCONF to IA-stations that are in factory-default state.

4.8.6.3 Verification Support Mechanisms

4.8.6.3.1 General

Subclause 4.8.6.3 considers mechanisms that support device identity verification during online interactions with IA-stations.

4.8.6.3.2 Secure Transports

Sending information in plain form over a protected channel, e.g., ietf-hardware YANG module contents via NETCONF-over-TLS protects the transferred information during its transit through the network but does not vouch for the correctness of the received information e.g., the mfg-name value.

4.8.6.3.3 Secure Information

Protecting information objects by means of cryptographic checksums allows to verify the authenticity and integrity of the provided information. Cryptographic checksums may use

1138 symmetric or asymmetric schemes. In case of asymmetric schemes, raw and self-signed public
1139 keys need to be distinguished from CA-signed public keys.

1140 Asymmetric schemes with CA-signed public keys are preferable for the verifiable device identity
1141 use case: claimants and verifiers share a public key; the claimant possesses the corresponding
1142 private key. The establishment and storage of the shared public keys uses public key
1143 certificates. For this approach self-signed CA certificates are to be established in an authentic
1144 manner. Their amount is independent from the number of verifiers (CNCs) as well as claimants
1145 (IA-stations).

1146 **4.8.6.3.4 IDevID and LDevID Credentials**

1147 IDevID and LDevID credentials are specified by IEEE Std 802.1AR. These objects are
1148 comprised of a certification path and a private key. The certification path encompasses an end
1149 entity certificate which contains verifiable device identity in a CA-signed form. The device
1150 identity verification happens after validating the certification path (IETF RFC 5280) and
1151 checking the proof-of-possession for the private key (IETF RFC 5246 in case of TLS 1.2). The
1152 certification path validation demands trust anchors as input arguments (IETF RFC 5280, 6.1.1
1153 input argument (d)).

1154 Two types of credentials are distinguished by IEEE Std 802.1AR:

- 1155 • IDevIDs are issued by device manufacturers. They represent an initial identity as it is known
1156 at device production-time. The initial device identity is not locally significant: it cannot
1157 contain deployment-specific information such as DNS names or IP addresses.
- 1158 • LDevIDs are issued by other actors e.g., a device user. They represent a locally significant
1159 device identity: they can contain deployment-specific information e.g., DNS names or IP
1160 addresses.

1161 IEEE Std 802.1AR uses signature suites to describe the subject public key and the signature
1162 fields in IDevID and LDevID certification paths. This notion is different from TLS cipher suites.

1163 NOTE IDevID and LDevID credentials also serve purposes beyond secure device identity, for instance the
1164 realization of secure transports. This facilitates the use case of NETCONF/YANG security setup from factory default
1165 state.

1166 **4.8.6.3.5 IDevID Items beyond IEEE Std 802.1AR**

1167 IEEE Std 802.1AR represents the initial device identity as serialNumber (OID 2.5.4.5) attribute
1168 in the subject field of the EE certificate. Its value provides the serial number of the device. This
1169 value is required to be unique within the domain of significance of the EE certificate issuer. The
1170 serialNumber attribute is an optional capability. This allows to verify following identity items:

- 1171 • certificate issuer (not necessarily: manufacturer) by issuer field (data type: ASN.1 Name)
- 1172 • if present: device instance by serialNumber value (data type: ASN.1 PrintableString).

1173 NOTE This verification can happen after certification path validation (see IETF RFC 5280) and the proof-of-
1174 possession checking for the private key (see IETF RFC 5246 in case TLS 1.2).

1175 The following bullet points describe options for verifying the device identity of IA-stations in
1176 factory default state. It also identifies informational items needed for the corresponding checks:

- 1177 • IA-station manufacturer check: using names that identify IA-station manufacturers e.g., mfg-
1178 name in ietf-hardware YANG module
- 1179 • IA-station type check: using attributes that identify IA-station types e.g., model-name, hw-
1180 revision, description in ietf-hardware YANG module
- 1181 • IA-station instance check: using values that identify IA-station instances e.g., serial-num in
1182 ietf-hardware YANG module.

1183 The following model described in the bullet points applies to the verification of the initial device
1184 identity of IA-stations:

- 1185 • the set of to-be-conducted checks is determined by IA-station and CNC users

- an IA-station uses IDevID credentials to prove its device identity. The checking happens by means of online interactions in the operational network. It happens automatically and is done by CNCs. This does not depend on configuration-domain external repositories
- other stakeholders e.g., middleware/application consortia or individual manufactures are allowed to additionally express information items in IDevID credentials to reflect their device identity model. CNCs do not assess such additional information.

4.8.6.3.6 Device Identity Representation in IDevID and LDevID Credentials

The best practices for representing verifiable device identity information in IDevID and LDevID credentials are.

- Corresponding information (actual values or references to them) appears in EE certificates:
 - IDevID EE certificates bind initial device identity items that are known by the device manufacturer at production time e.g., mfg-name.
 - LDevID EE certificates bind locally significant device identity items that are known by other actors such as device users e.g., DNS names or IP addresses. They may also bind initial device identity information.
 - Items that encode device naming information appear in the subjectAltName extension.
- NOTE This is required by IETF RFC 5280, 4.2.1.6. It is also backed by IETF RFC 6125, 2.3.
- A binding can take one of following forms. Multiple forms can appear in one EE certificate:
 - By-value: the verifiable device identity information is represented by its value inside the IDevID resp. LDevID EE certificate. Examples are:
 - the product serialNumber in IDevID credentials (IEEE Std 802.1AR)
 - the hostname of the NETCONF/YANG server in LDevID-NETCONF credentials (IETF RFC 7589 and IETF RFC 6125)
 - By-ref: the verifiable device identity information is represented by a reference inside the IDevID resp. LDevID EE certificate, not by its value:
 - The actual value may be provided by the device itself or by a device-external source.
 - If it is provided in form of an unprotected information object, then the reference object that is embedded to EE certificates should include a digest value.

5 Conformance

5.1 General

A claim of conformance to this document is a claim that the behavior of an implementation of an IA-station (see 5.5, 5.6) with its bridge components (see 5.7, 5.8) and end station components (see 5.9, 5.10) meets the mandatory requirements of this document and may support options identified in this document.

5.2 Requirements terminology

- Requirements terminology is provided in the ISO/IEC Directives Part 2:2021, Clause 7. This document can be found at www.iec.ch/members_experts/refdocs.
- The Profile Conformance Statement (PCS) proformas (see Annex A) reflect the occurrences of the words “shall,” “may,” and “should” within this document.
- The document avoids needless repetition and apparent duplication of its formal requirements by using is, is not, are, and are not for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by can. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by cannot. The word allow is used as a replacement for the phrase “Support the ability for,” and the word capability means “can be configured to.”